In the Description:

Page 7, lines 5 to 11, cancel " These ... system." and substitute therefor:

--These and other objects and advantages of the Invention will become more apparent from the following detailed description taken in conjunction with the accompanying drawing ~~drawings~~ wherein:

Figure 1 represents an algorithm for the n-dimensional biometrics access control system using speech in accordance with the invention.

~~Fig. 1 represents a model of the n-dimensional biometrics access control system using speech in accordance with the invention;~~

~~Fig. 2 illustrates a simultaneous record prior to matching whereby a unique date/time identifier and hash of the entire record is imbedded in each object; and~~

~~Fig. 3 illustrates a schematic view of the n-dimensional biometrics access control system.~~ - -

Page 7, lines 12 to 23, change " The proposed...system." to

--The proposed security scheme improves security over past methods through a system challenge response method of randomly generated phrases. Each time the user is authenticated, a random biometric identifier is created unique to the user at that distinct moment. Upon access, a distinct and random biometric tied uniquely to the user provides the basis for a highly secure system. This prevents an unauthorized user from utilizing the traditional hacking techniques of cracking, stealing information and system penetration with access information at another time. Recording or theft of voice samples or properties do not help a hacker because it would be highly unlikely to reconstruct the random phrase on the fly given the short period of time for which the user and user

terminal must respond. The methodology also prevents an "authorized agency" from sending around authentication information that could be used by other third parties without the user directly knowing. The solution addresses security fraud issues that surround token methods such as with ~~Microsoft's~~ the passport authentication and authorization system of the Microsoft Corporation.—

Page 8, lines 8 to 17, change "A second...control." to

—A second way In which the proposed n-dimensional security scheme improves privacy is through the use of language sets. Language sets are subsets that apply to the same rules and knowledge of the overall language but encompass a subject area that gives the user an intuitive understanding of the system and some control over his or her participation with the system. Because the phrases are generated within a language set there must be enough variation of words, types of words and types of phrase structures to generate the kind of randomness and security required. Language sets give the user and the organization the option of moving users to different language sets or deleting them from the language set forever. It is likely that a user will remember having been in the "Fashion" or "Sports" language set many years down the road since it is so intuitive. This addresses public concerns such as the ~~Microsoft's~~ MICROSOFT® passport token which users distrust and cannot easily and intuitively control.--

Page 11, lines 3 to 7, change " Figure 1....model." to

--Figure 1 represents ~~a model~~ an algorithm of the n-dimensional model ~~idea~~ at the concept level using speech. The assumption is that the Human Input ~~x~~ which, in this case, is the vocalization of a Phrase *, is equal to the Biometric Input *. The biometric matching process results and human recognition matching process results are therefore

~~inexplicably~~ inextricably tied. It is the union of Human and Biometric processes versus either performed separately that is the essence of the model and the basis for the benefits of an n-dimensional ~~n-dimensional~~ model.—

Page 11, lines 8 to 16, change " The ...technique." to

-- The proposed security scheme uses this model as a basis for the system generated, as well as user generated, phrases. The objective of a practical system today is that the system generates random phrases where n goes minimally to 1,000 phrases and the user chooses phrases where n likely goes from 0 to 5 depending on user preference. A hacker would have great difficulty recreating one of the possible 1,000 phrases on the fly as the security system design is constructed herein. This application discusses the use of language, language sets and practical examples but does not address the vast subject encompassing the natural language processing possibilities inherent in the function sets ~~referred to in Figure 1~~. The full potential of these function sets are beyond the scope of the application and represent further areas that refine such a security technique. --

Page 12, line 1, cancel "The ...below."

Page 15, lines 8 to 17, change "The ..user." to

--The authentication process begins when a ~~remoter~~ remote user requests access, for example to their AOL® accounts and services. During the initial user request for access, the user makes a claim that represents who they are. The claim information could be through a keyboard input of a PIN, speech input of PIN or other identification information such as an account number, identification of the cell phone ID provided by cell phone provider or any other method that facilitates the users initial

claim as to who they are. Said claim information could be digitally signed and/or encrypted. The main controller validates initial user claim information and performs random generation of a challenge phrase as described herein and optionally associated encryption and/or digital signature keys to be used to protect authentication information described herein across the network. A user can also be requested to speak a phrase determined by the user.–

Page 15, lines 18 to 22, chnage " As ..process." to

—~~As shown in Figure 3, the~~ The proposed security system comprises at least one user terminal and a controller gateway function, which determines access, based on matching results. The gateway performs management and control functions associated with matching or recognition, enrollment, random phrases, language sets, database security and encryption. Such a controller could be associated with single sign on systems to further the power and reach of the authentication process.—

Page 17, between lines 12 and 13 insert the following:

-- Referring to Fig. 1, in a first step 10 when a user makes a request for system access, the controller generates a challenge phrase, i.e. the n-dimensional parameter, from a number (n) of random challenge phrases.

In a second step 11, the controller requests the user to speak the phrase, collects the response made by the user and generates a signal representative of the spoken phrase, i.e. voice features representative of the user's voice print and the words that are spoken.

This signal is then processed by automatic speech recognition (ASR) for ASR matching 12 to validate the the voice information used for speaker recognition. If

validated, a signal to that effect is generated.

The signal representative of the spoken phrase is also processed to verify the voice information used for speech recognition (Verification matching 13). If validated, a signal to that effect is generated.

If the two validation signals (from the ASR matching and the Verification matching) match each other, an acceptance of the user to the system is made. If the two validation signals do not match each other, the user is rejected and acess to the system is denied to the user. --